RSAC™ 2025 Conference

Many Voices.
One Community.

SESSION ID: HT-R03

Group Discussion

Continue the conversation on the new RSAC Community Platform.

RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: HT-R03

Non-Human Identity Security Insights from 800+ Security Professionals

John Yeoh
Chief Scientific Officer, CSA

Tal Skverer
Head of Research, Astrix Security

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Agenda for NHI Insights

01 Define NHIs

02 NHIs Evolved

03 NHIs Exposed

04 Industry Validation

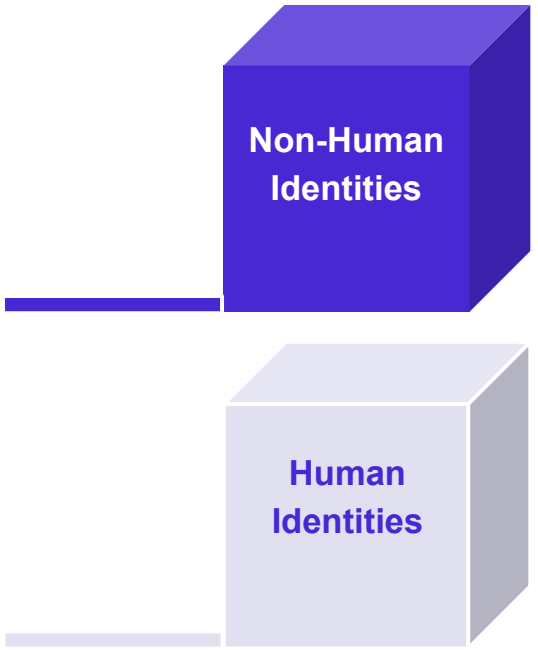
05 Apply Today's Insights

06 Future Proof NHI Security

What are Non-Human Identities?

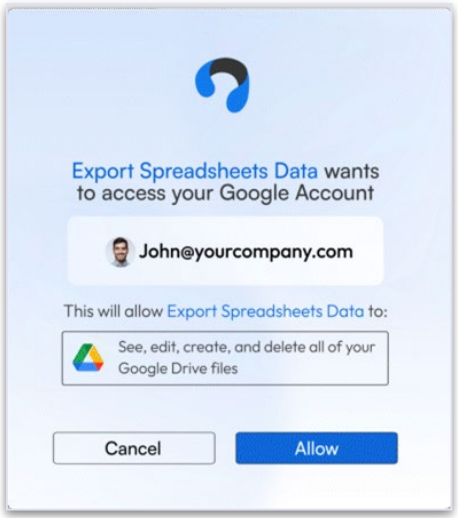
"Programmatic access to a process or data where a human is not required to be involved."

- Users
- API Keys
- Service Accounts
- Access Keys
- Cloud Roles
- Personal Access Tokens
- Webhooks
- OAuth Apps
- SSH Keys
- Employees

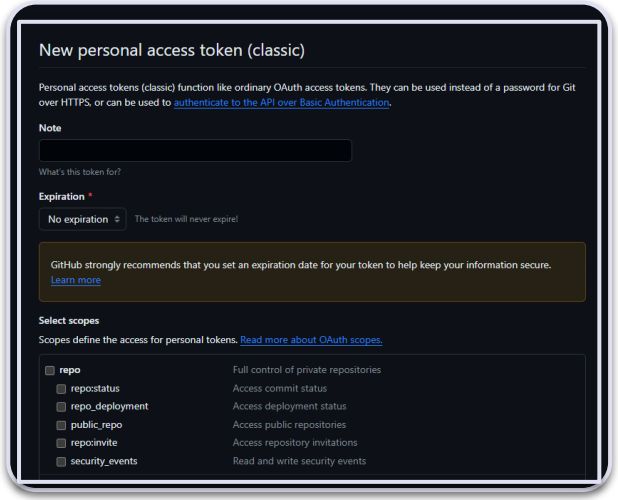


Evolution of NHI Creation

Humans authorizing NHIs


Export Spreadsheets Data wants to access your Google Account
John@yourcompany.com
This will allow Export Spreadsheets Data to:
See, edit, create, and delete all of your Google Drive files
Cancel
Allow

Humans creating NHIs


New personal access token (classic)
Personal access tokens (classic) function like ordinary OAuth access tokens. They can be used instead of a password for Git over HTTPS, or can be used to authenticate to the API over Basic Authentication.
Note
What's this token for?
Expiration *
No expiration
The token will never expire!
GitHub strongly recommends that you set an expiration date for your token to help keep your information secure.
Learn more
Select scopes
Scopes define the access for personal tokens. Read more about OAuth scopes.
repo
Full control of private repositories
repo:status
Access commit status
repo_deployment
Access deployment status
public_repo
Access public repositories
repo:invite
Access repository invitations
security_events
Read and write security events

NHIs creating NHIs

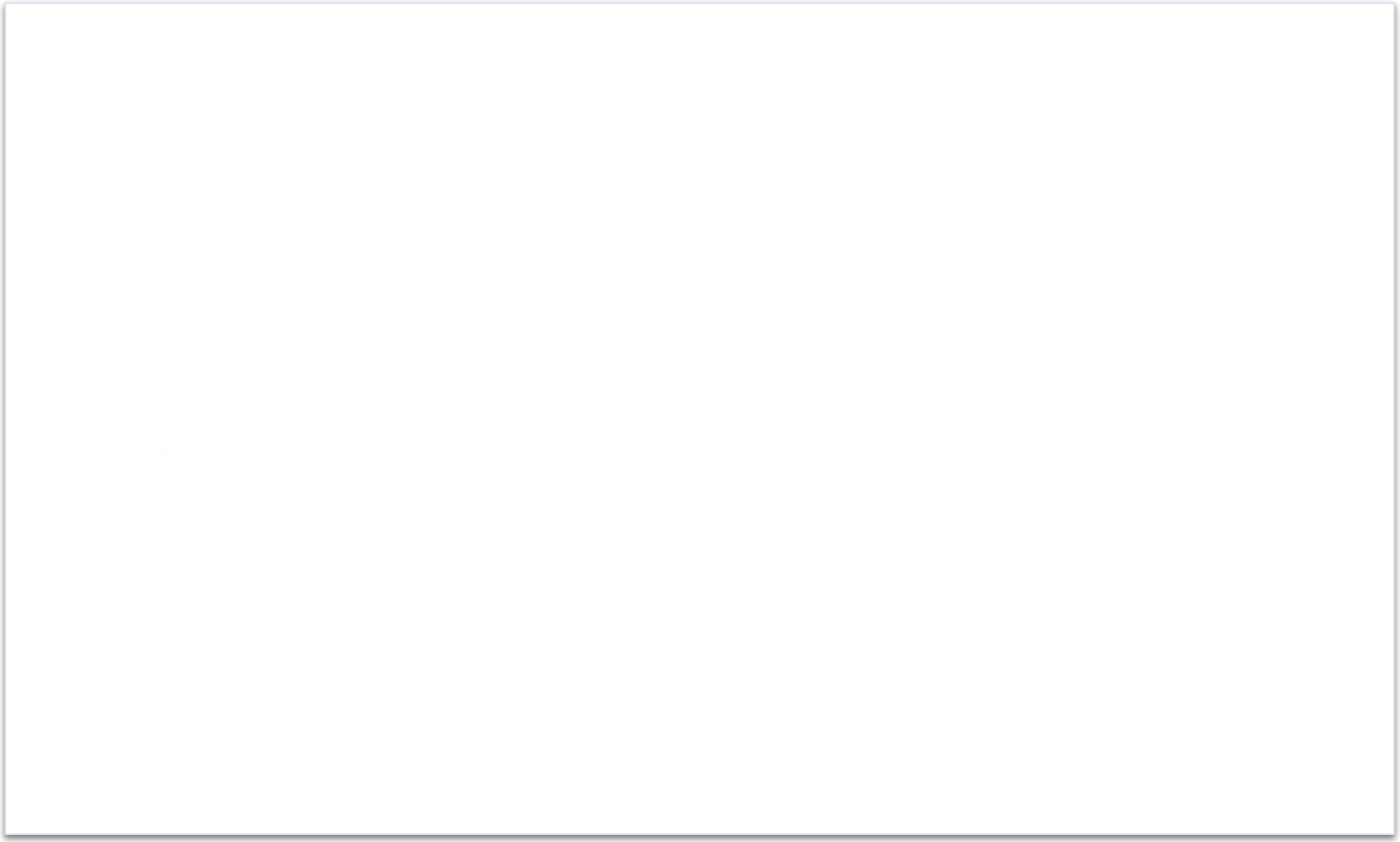
```
provider "aws" {
  region = "us-east-1"
}

resource "aws_iam_user" "new_user" {
  name = "dynamo-db-bot"
}

resource "aws_iam_access_key" "new_user_access_key" {
  user = aws_iam_user.new_user.name
}
```

1,000 employees = **45,000** non-human identities

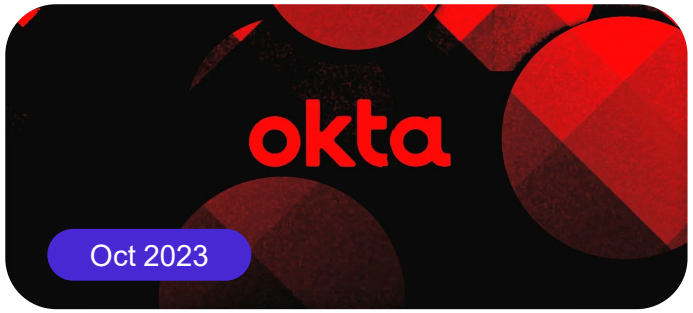
Agentic AI – A Breeding Ground for NHIs



Attackers Targeting NHIs

It Only Takes **One Key to the Kingdom**

Chinese hackers breach US treasury using stolen API key



Okta's support system was breached via stolen credentials

CI/CD pipeline attack exposes unauthorized access to secrets

Dropbox says hackers stole customer data, auth secrets from eSignature service

Snowflake Breach Exposes 165 Customers' Data in Ongoing Extortion Campaign

Nation-state attackers compromised cloud-native system identities

CSA Security Report: The State of NHI Security

Industry Insights and Validation

Goals and Objectives

- Main concerns
- Top challenges
- Attacks and Vulnerabilities
- NHI incidents
- Current NHI strategies
- NHI Security opportunities

800+ Participants

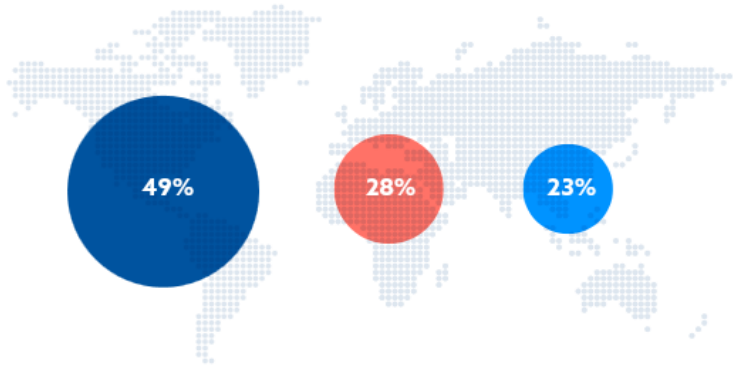
- Security professionals
- C-suite
- Directors and managers
- Architects and developers
- Americas, EMEA, APAC

NHI Security Report: Demographic

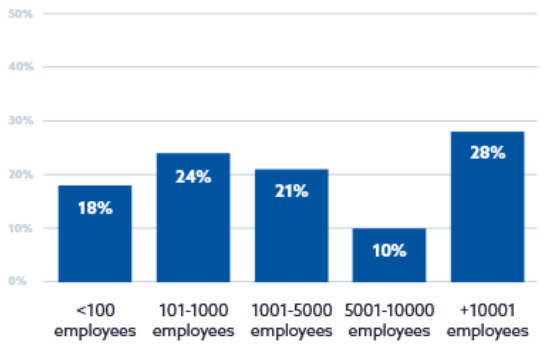
Demographics

The survey was conducted online by CSA in June 2024 and received 818 responses from IT and security professionals from organizations of various sizes and locations.

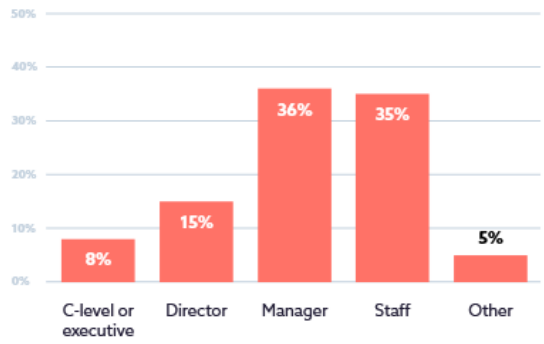
What region of the world are you located in?



What is the size of your organization?



What best describes your job level?



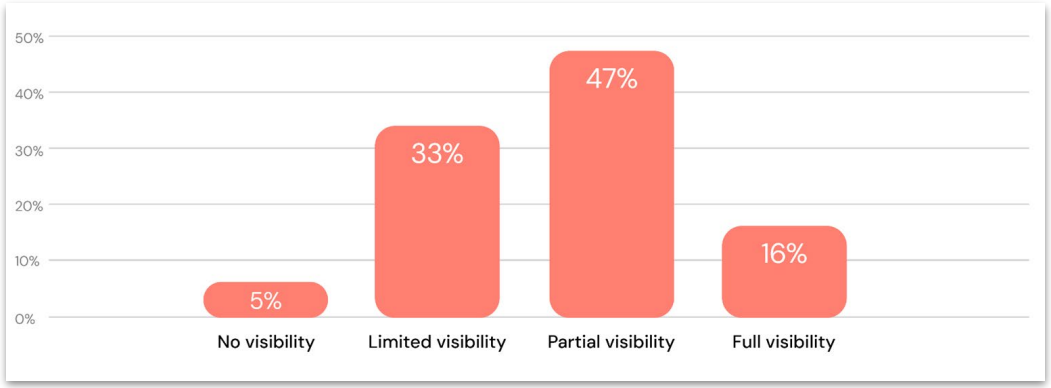
Key Finding #1:

Struggling With the Basics of NHI Security

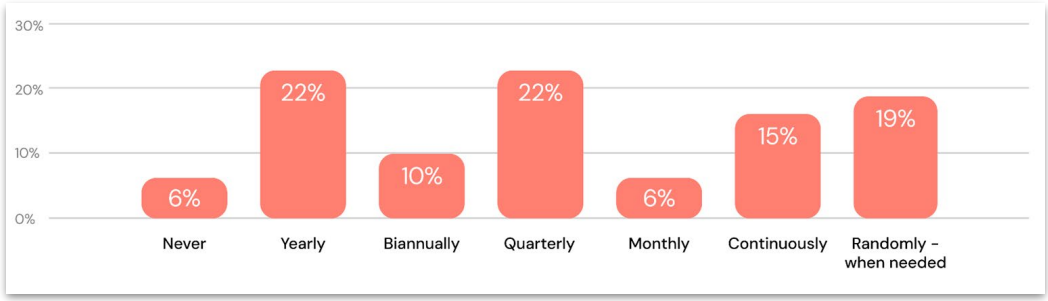
Most challenging aspects of NHI management

32%	Service accounts	21%	Managing the secrets lifecycle
25%	Auditing & Monitoring	20%	IAM roles
25%	Access & privileges	19%	Vendor-owned APIs
24%	Discovering NHIs	18%	Managing requests for third-party tools & services
21%	Policy Enforcement		

Visibility levels into third-party vendor connected by OAuth apps



Frequency of review for service account permissions



Observation and Application

Service Account Pitfalls, Visibility

Most challenging aspects of NHI management

32%	Service accounts	21%	Managing the secrets lifecycle
25%	Auditing & Monitoring	20%	IAM roles
25%	Access & privileges	19%	Vendor-owned APIs
24%	Discovering NHIs	18%	Managing requests for third-party tools & services
21%	Policy Enforcement		

Service Account Types

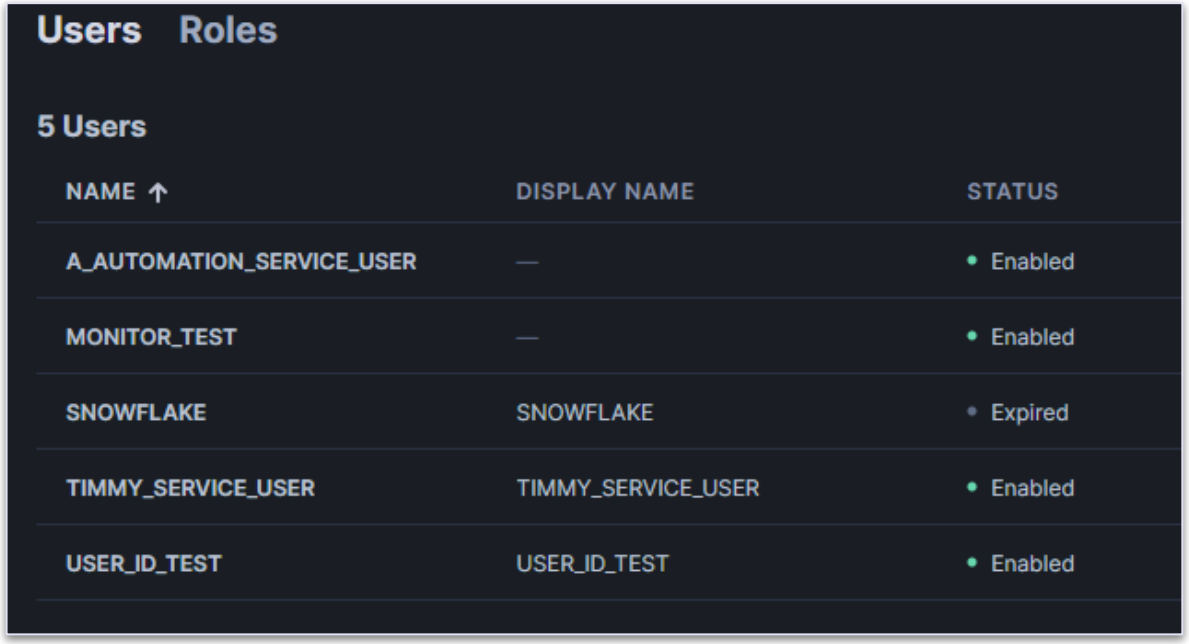
1. User Service Accounts
   a. Human users converted into NHIs
2. Cyborgs
   a. Identity used both by Human and Non-Human
3. Built-in Service Accounts
   a. NHI-designated users baked into the platform

Observation and Application

User Service Accounts: Common Difficulties

User Service Accounts

- Lack fine-grained permissions
- Difficulty to rotate password
- Rely on irrelevant human-oriented security protocols
- Missed by NHI monitoring tools



Observation and Application

User Service Account vs. Managed Identity

User Service Account

- Never expiring password
- Hard to distinguish from normal user
- No MFA
- Credentials stored statically

Managed Identity

- Short lived access token
- Password derived from certificate
- Auto rotated every 3 months
- Accessible only from specific resource(s)
- No credential is stored on the machine

Observation and Application

User Service Account vs. Managed Identity

```python
from azure.identity import UsernamePasswordCredential
from azure.mgmt.resource import ResourceManagementClient

# User credentials
TENANT_ID = "your-tenant-id"
CLIENT_ID = "your-client-id"
USERNAME = "your-username@example.com"
PASSWORD = "your-strong-password"

# Authenticate using the user account
credential = UsernamePasswordCredential(tenant_id=TENANT_ID, client_id=CLIENT_ID, username=USERNAME, password=PASSWORD)

# Azure subscription ID
SUBSCRIPTION_ID = "your-subscription-id"

# Create a Resource Management Client
resource_client = ResourceManagementClient(credential, SUBSCRIPTION_ID)

# List all resource groups in the subscription
resource_groups = resource_client.resource_groups.list()

print("Resource Groups:")
for rg in resource_groups:
    print(f"- {rg.name}")
```

```python
from azure.identity import ManagedIdentityCredential
from azure.mgmt.resource import ResourceManagementClient

# Azure subscription ID
SUBSCRIPTION_ID = "your-subscription-id"

# Authenticate using Managed Identity (system-assigned or user-assigned)
credential = ManagedIdentityCredential()

# Create a Resource Management Client
resource_client = ResourceManagementClient(credential, SUBSCRIPTION_ID)

# List all resource groups in the subscription
resource_groups = resource_client.resource_groups.list()

print("Resource Groups:")
for rg in resource_groups:
    print(f"- {rg.name}")
```

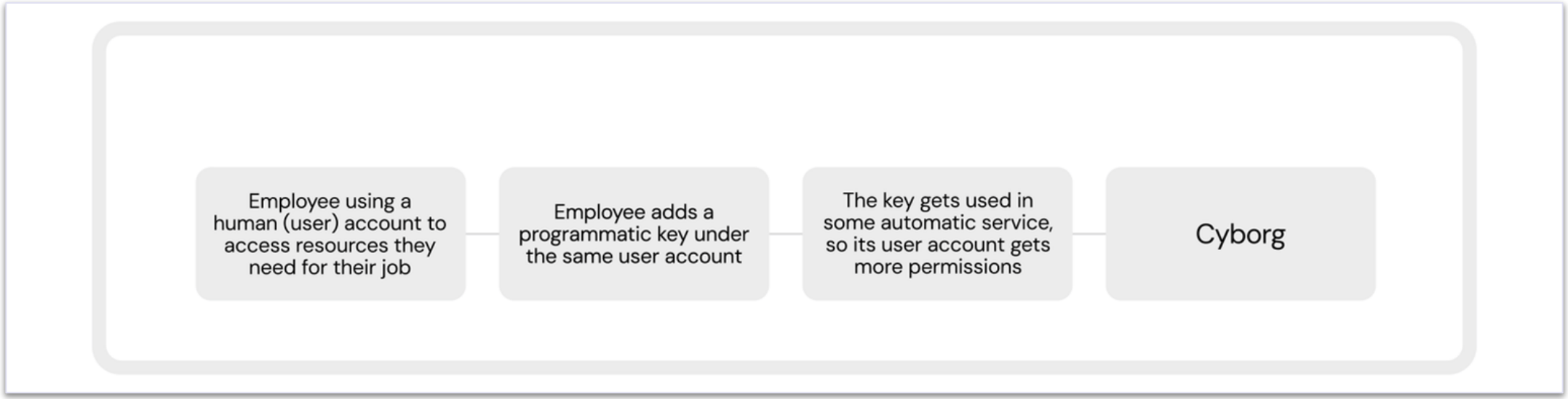
The variables necessary to authenticate as a user

Observation and Application

Cyborg Accounts: Common Difficulties

Cyborg accounts

- Bloated permissions
- Usually non-expiring
- Create offboarding issues & operational disruptions

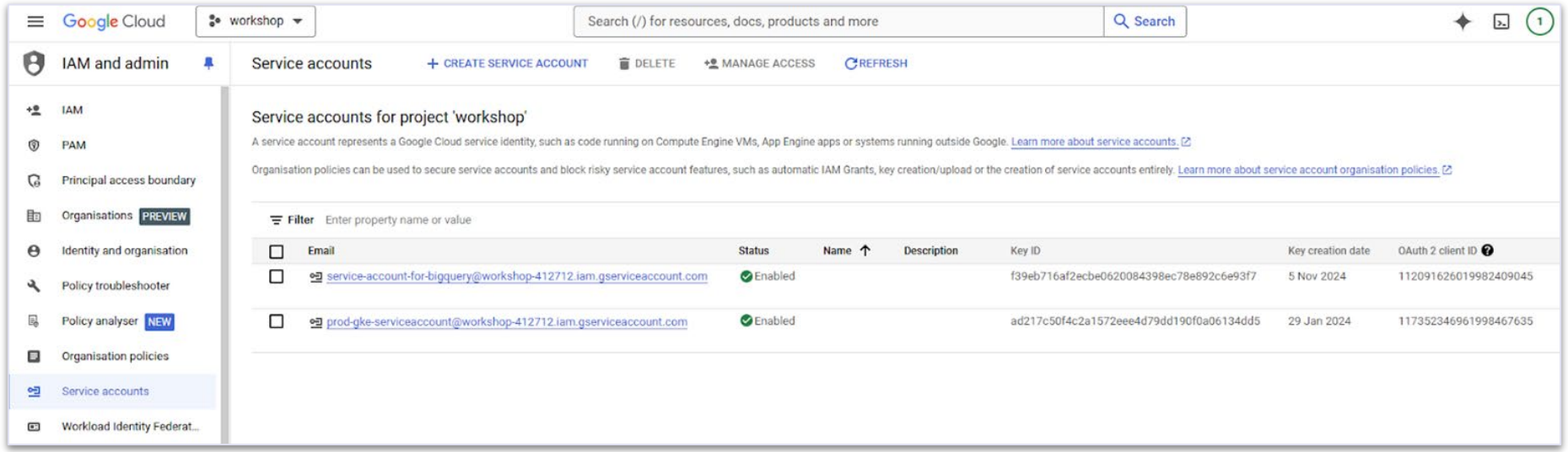

Employee using a human (user) account to access resources they need for their job
Employee adds a programmatic key under the same user account
The key gets used in some automatic service, so its user account gets more permissions
Cyborg

Observation and Application

Built-in Service Accounts: Common Difficulties

Built-in service accounts

- Usually have automatically-expiring keys
- Use long cryptographic keys instead of short passwords
- Support fine-grained permissions

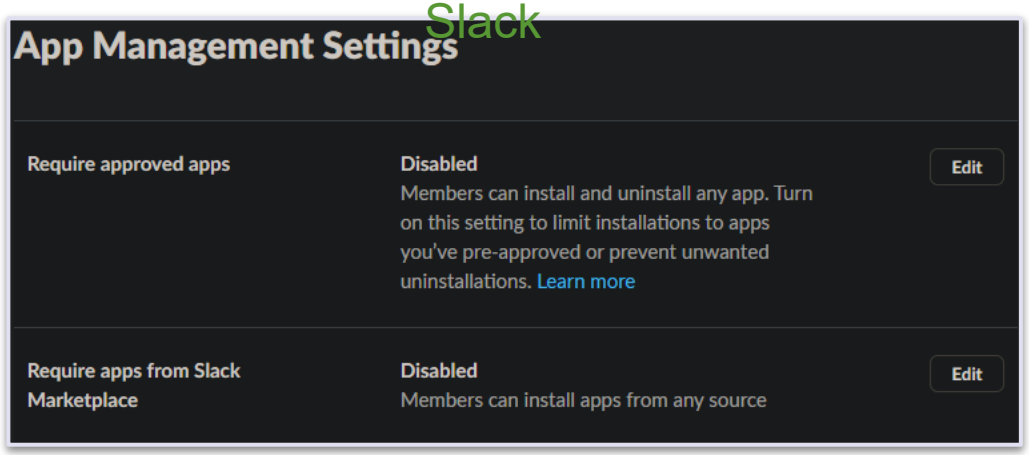

Google Cloud
workshop
Search (/) for resources, docs, products and more
Search
IAM and admin
Service accounts
CREATE SERVICE ACCOUNT
DELETE
MANAGE ACCESS
REFRESH
IAM
PAM
Principal access boundary
Organisations PREVIEW
Identity and organisation
Policy troubleshooter
Policy analyser NEW
Organisation policies
Service accounts
Workload Identity Federat...
Service accounts for project 'workshop'
A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps or systems running outside Google. Learn more about service accounts.
Organisation policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload or the creation of service accounts entirely. Learn more about service account organisation policies.
Filter Enter property name or value
Email Status Name Description Key ID Key creation date OAuth 2 client ID
service-account-for-bigquery@workshop-412712.iam.gserviceaccount.com Enabled f39eb716af2ecbe0620084398ec78e892c6e93f7 5 Nov 2024 112091626019982409045
prod-gke-serviceaccount@workshop-412712.iam.gserviceaccount.com Enabled ad217c50f4c2a1572eee4d79dd190f0a06134dd5 29 Jan 2024 117352346961998467635

Observation and Application

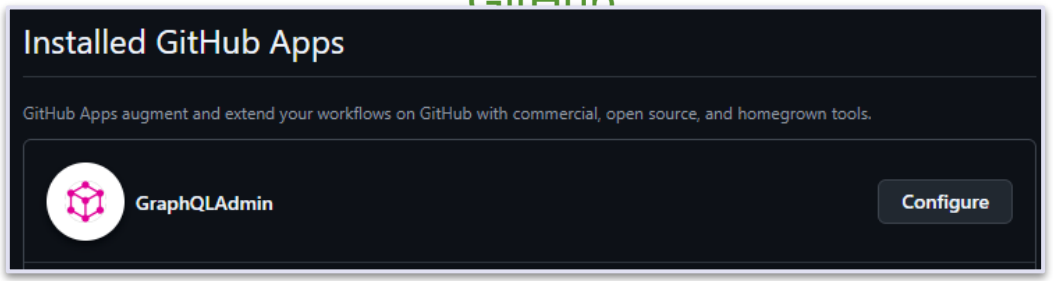
Third-Party OAuth Applications

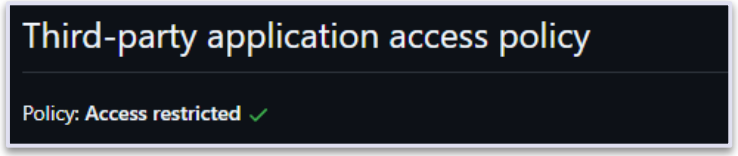
- Discovery - Visibility
- Policing
- Public Marketplaces

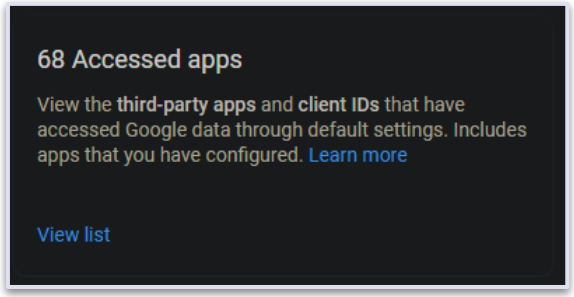
Slack


App Management Settings
Require approved apps
Disabled
Members can install and uninstall any app. Turn on this setting to limit installations to apps you've pre-approved or prevent unwanted uninstallations. Learn more
Edit
Require apps from Slack Marketplace
Disabled
Members can install apps from any source
Edit

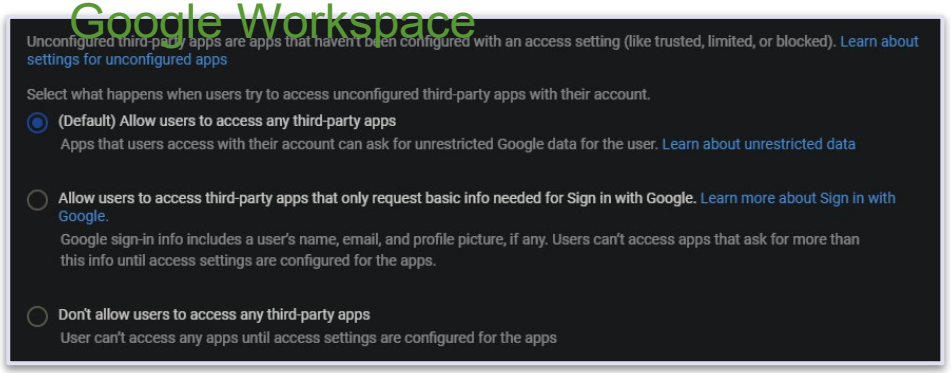
GitHub


Installed GitHub Apps
GitHub Apps augment and extend your workflows on GitHub with commercial, open source, and homegrown tools.
GraphQLAdmin
Configure




68 Accessed apps
View the third-party apps and client IDs that have accessed Google data through default settings. Includes apps that you have configured. Learn more
View list

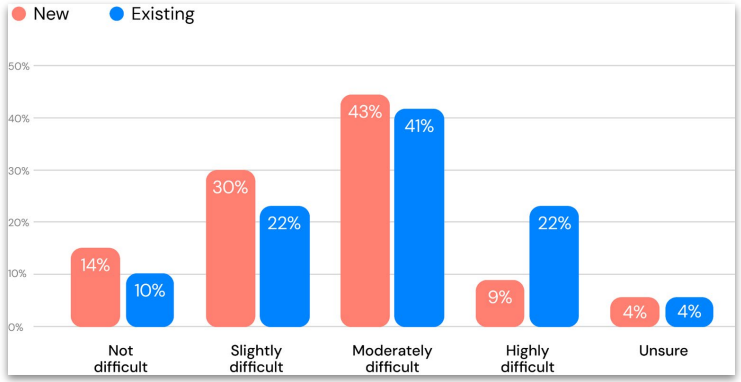
Google Workspace


Unconfigured third-party apps are apps that haven't been configured with an access setting (like trusted, limited, or blocked). Learn about settings for unconfigured apps
Select what happens when users try to access unconfigured third-party apps with their account.
(Default) Allow users to access any third-party apps
Apps that users access with their account can ask for unrestricted Google data for the user. Learn about unrestricted data
Allow users to access third-party apps that only request basic info needed for Sign in with Google. Learn more about Sign in with Google.
Google sign-in info includes a user's name, email, and profile picture, if any. Users can't access apps that ask for more than this info until access settings are configured for the apps.
Don't allow users to access any third-party apps
User can't access any apps until access settings are configured for the apps

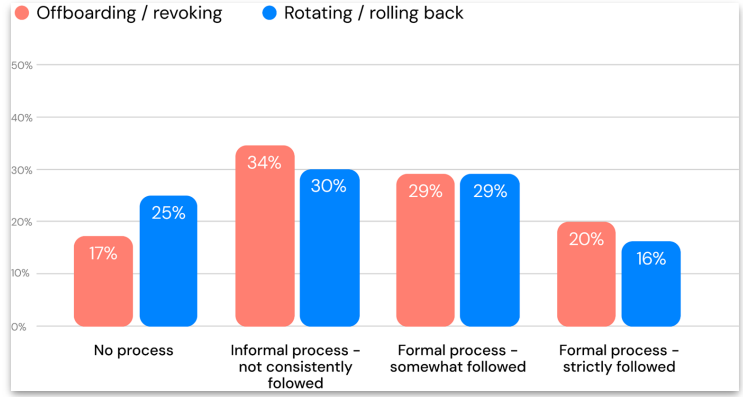
Key Finding #2:

Processes Lacking For Managing NHI Lifecycle

Difficulty levels of managing permissions for new versus existing service accounts



Difficulty levels of managing permissions for new versus existing service accounts



Timeline for API key offboarding versus rotating / rolling back

Observation and Application

Applying Minimal Permission to Existing NHIs

AWS Identity and Access Management Access Analyzer provides the following capabilities:

- IAM Access Analyzer external access analyzers help identify resources in your organization and accounts that are shared with an external entity.
- IAM Access Analyzer unused access analyzers help identify unused access in your organization and accounts.
- IAM Access Analyzer validates IAM policies against policy grammar and AWS best practices.
- IAM Access Analyzer custom policy checks help validate IAM policies against your specified security standards.
- IAM Access Analyzer generates IAM policies based on access activity in your AWS CloudTrail logs.

GCP - Policy Intelligence

Improve your policies

You can improve your IAM allow policies by using role recommendations. Role recommendations help you enforce the principle of least privilege by ensuring that principals have only the permissions that they actually need. Each role recommendation suggests that you remove or replace an IAM role that gives your principals excess permissions.

Role	Security insights
Owner	4565/4569 excess permissions
VPC Service Controls Troubleshooter Viewer	21/21 excess permissions
Custom Role	4/4 excess permissions
Service Account Token Creator	9/9 excess permissions and 31 service account impersonations
Service Account User	5/5 excess permissions and 31 service account impersonations

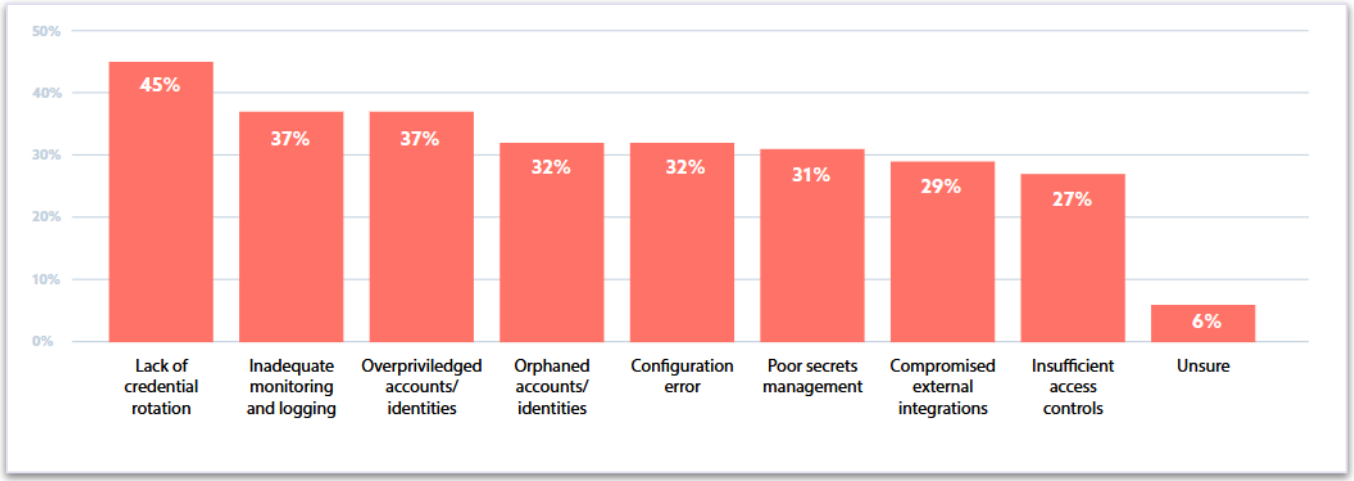
Key Finding #3:

Fragmented Approaches Lead to Security Incidents

Most challenging aspects of NHI management

58%	Identify & Access Management (IAM)
54%	Privileged Access Management (PAM)
40%	API security
38%	Zero trust/least privilege
36%	Secrets Management tools
35%	Behavioral Analytics & Anomaly detection
35%	Auditing & monitoring
34%	Cloud Access Security Broker (CASB)
23%	Workload identity management
22%	Automated Discovery & Management tools
20%	Custom Scripts/Tools
18%	Machine identity protection
14%	Robotic process automation (RPA)
2%	We do not use any specific technology

Causes of NHI security incidents



Observation and Application

Authentication, privileges, key rotation, lifecycle

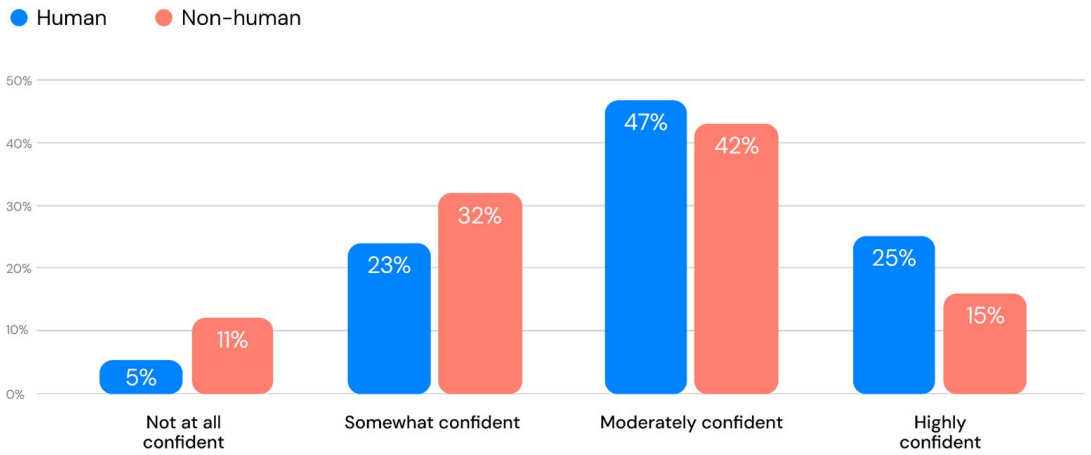
- Why rotating credentials is so hard?
  1. Need to manually update all consumers
  2. Need to keep track of all credentials

- How to solve?
  1. Change consumers to access credentials from vault
  2. Transformation to credential-less authentication

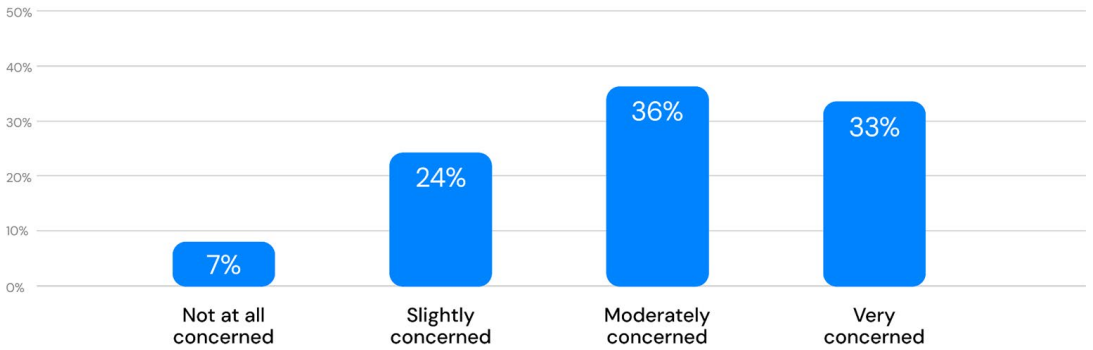
Key Finding #4:

High Anxiety, Low Confidence When Securing NHIs

Confidence levels in human identity vs NHI attack prevention



Concern levels about NHI as an attack vector



Observation and Application

Lack of confidence comes from gap in understanding

- Educating staff, not just providing tools
- CSA Working Groups
  - Identity Working Group – NHI
  - Zero Trust Working Group - Identity
  - https://cloudsecurityalliance.org/research/working-groups/
- Non-Human Identity Management Group
  - https://nhimg.org/

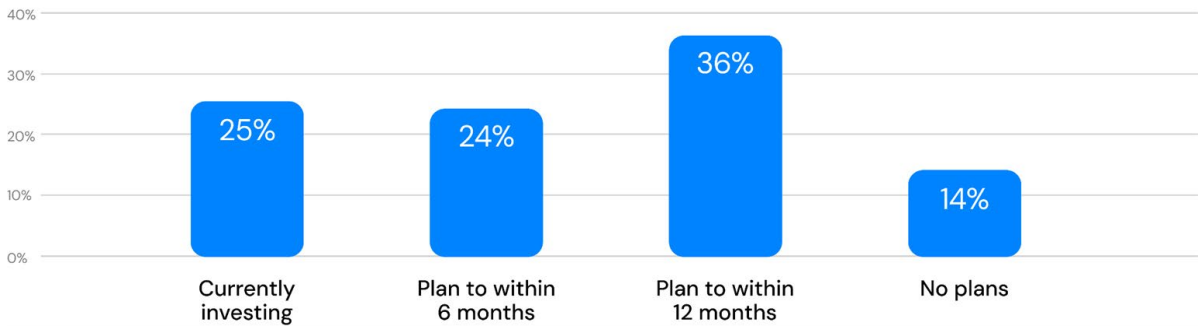
OWASP: Top 10 NHI Risks

CSA: NHI Security – The Complete Technical Guide

Key Finding #5:

NHI Security Capabilities and Opportunities Coming

Plans to invest in NHI security capabilities

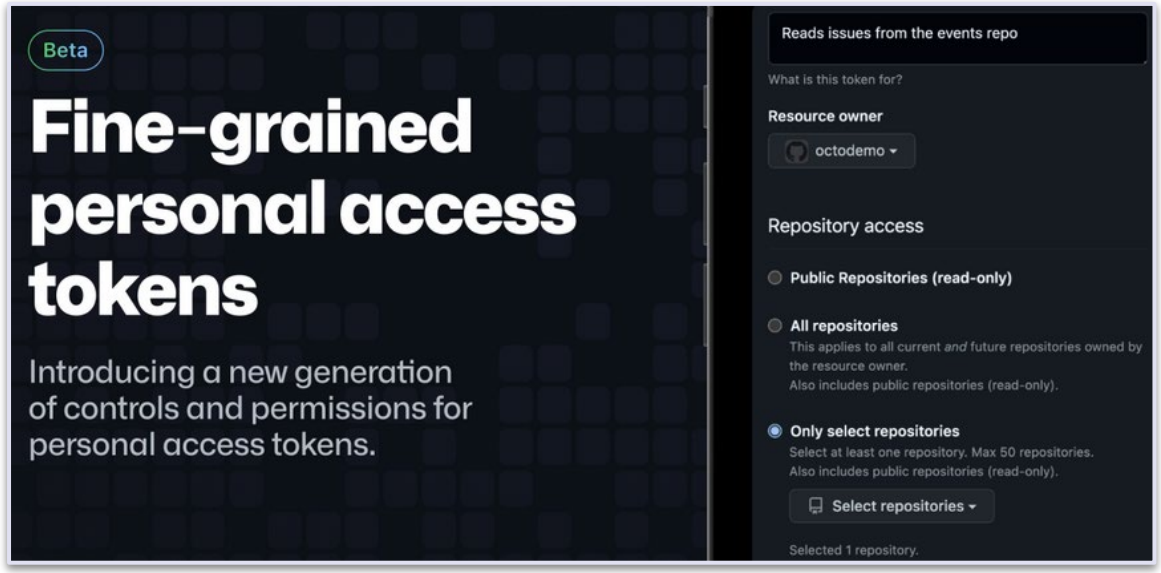


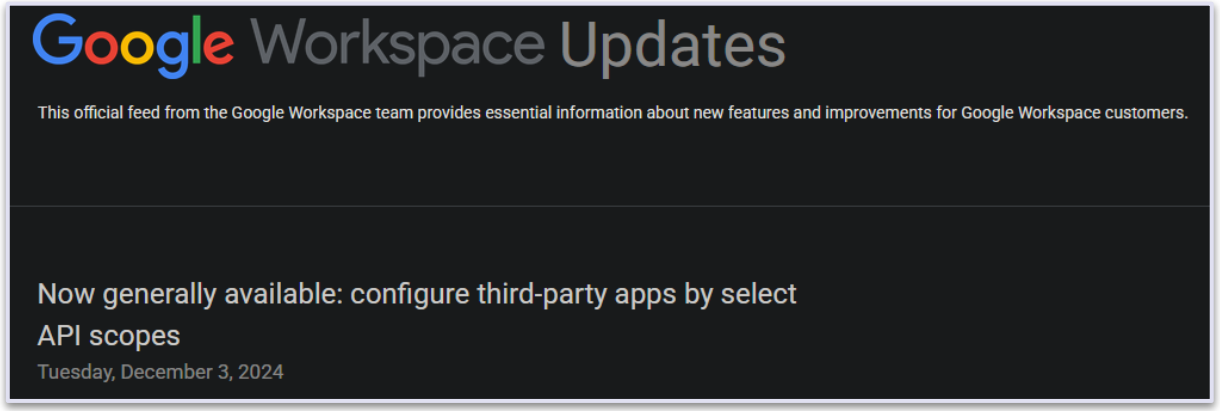
Which capabilities are needed for an NHI security tool?

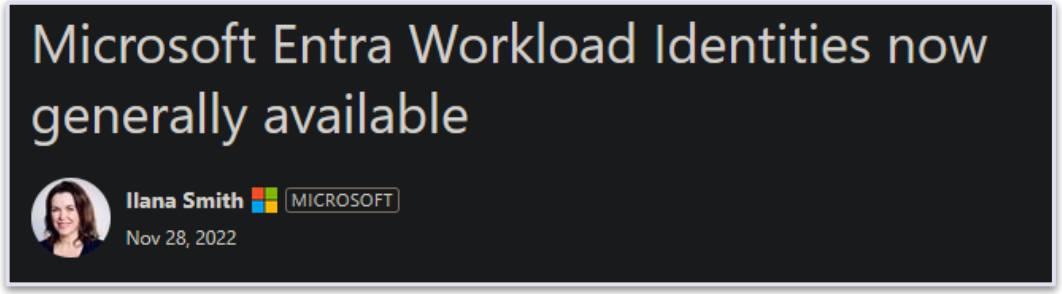
26%	Visibility into third-party vendors connected via OAuth apps	15%	Automated provisioning & de-provisioning of identities
26%	Management of the secrets lifecycle	14%	Audit & logging of NHIs
25%	Identity discovery	14%	Identity owners & consumers of NHIs
23%	Management of API keys	13%	Policy enforcement
22%	Managing permissions	13%	Incident response & remediation
22%	Tracking access behavior/anomaly detection	9%	compliance management
21%	Automate third-party connectivity	7%	Scalability
16%	Access control to sensitive information	1%	Use level of NHIs

Observation and Application

NHI security features today and tomorrow

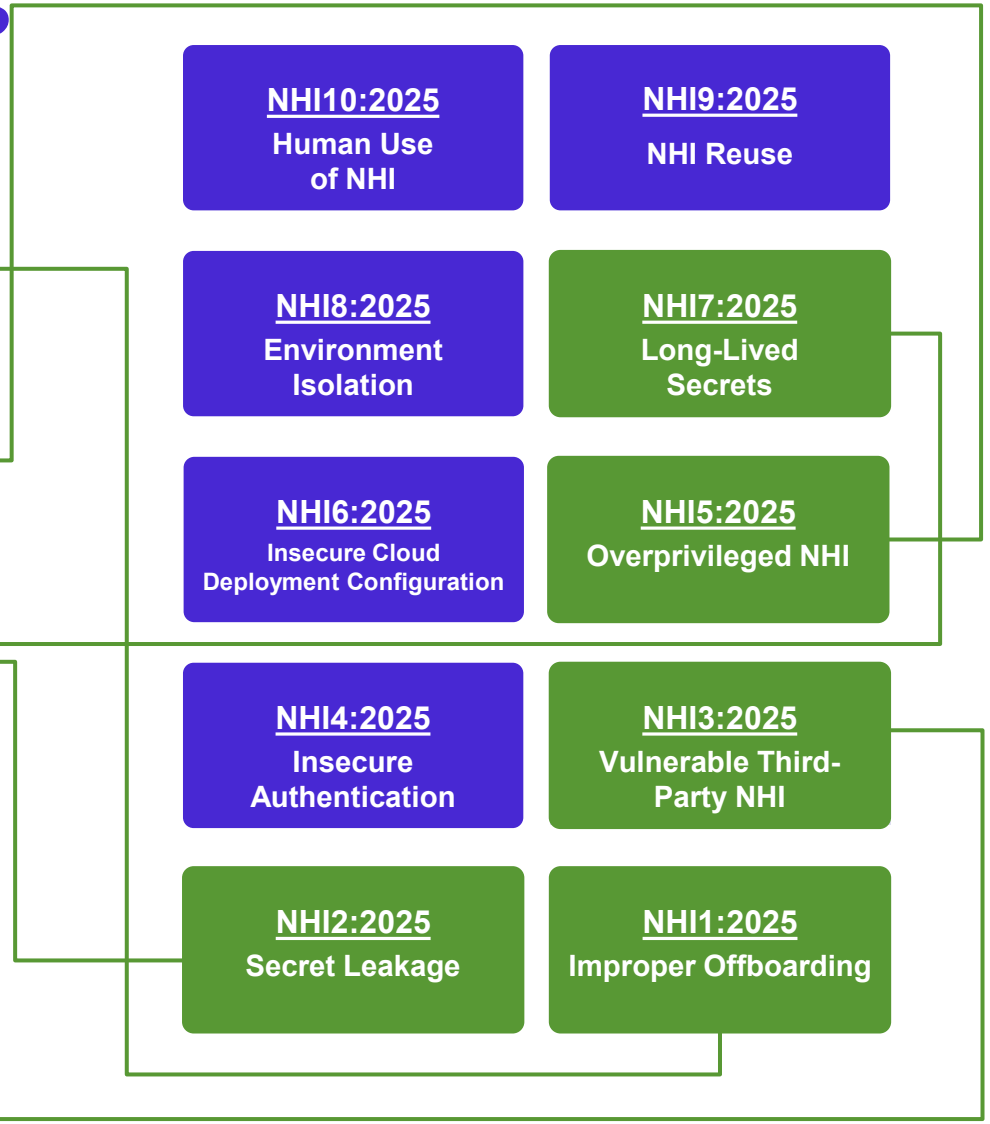

Beta
Fine-grained personal access tokens
Introducing a new generation of controls and permissions for personal access tokens.
Reads issues from the events repo
What is this token for?
Resource owner
octodemo
Repository access
Public Repositories (read-only)
All repositories
This applies to all current and future repositories owned by the resource owner.
Also includes public repositories (read-only).
Only select repositories
Select at least one repository. Max 50 repositories.
Also includes public repositories (read-only).
Select repositories
Selected 1 repository.


Google Workspace Updates
This official feed from the Google Workspace team provides essential information about new features and improvements for Google Workspace customers.
Now generally available: configure third-party apps by select API scopes
Tuesday, December 3, 2024



The OWASP Top 10 NHI Risks

- Over 50% of orgs don't have formal offboarding process
  (Risk #1)
- 37% of NHI incidents caused by overprivileged NHIs
  (Risk #5)
- 45% of NHI incidents caused by unrotated credentials
  (Risks #2 & #7)
- 38% of orgs have limited visibility into 3rd party NHIs
  (Risk #3)



Top Threats in Cloud - Deep Dive (2025 🔥)

Darkbeam (2023)

Threat Actor	Threats	Vulnerabilities
Internal Instances were exposed to the public internet, potentially due to binding the service to a public-facing IP address instead of a private or localhost IP or a default misconfiguration. **External** Prolonged exposure.	**TT7 - Accidental Data Disclosure** Public exposure of over 3.8 billion email-password combinations due to a misconfigured interface. However, no evidence of unauthorized exfiltration.	**TT3: Misconfiguration and Inadequate Change Control** An unsecured database configuration exposed sensitive data to the public. **TT2: IAM** Passwords stored in plain text or without sufficient encryption.

NHI Involvement

Misconfigured backend service
DevOps process with excessive access and no identity-based protection

Retool and Fortress (2023)

Threat Actor	Threats	Vulnerabilities
Internal Employee victim to combination of social engineering attacks, providing threat actor with credentials and MFA token. **External** Unknown threat actor infiltrated environment.	**Opportunistic** Threat actor used Retool's migration period to Okta, using phishing emails and credential harvesting,	**TT1 - Misconfiguration and Inadequate Change Control** Added a new MFA device for persistent access. **TT2 - IAM** Credential harvesting and obtaining authentication. **TT5 - Insecure Third-Party Resources** New features to Authenticator which led to MFA tokens being synced to the cloud

NHI Involvement

Service account credentials
Token/script misuse, long-lived credentials

Snowflake (2024)

Threat Actor	Threats	Vulnerabilities
TT11 - APT Organized Crime - Identified attacker and partners associated with hacking forums exploit and extort data.	**Data Theft** - Infostealer malware **Account Hijacking** of Snowflake accounts **Extortion** of victim organizations	**TT2 - IAM** Lack of MFA

NHI Involvement

Service account credentials
Token/script misuse, long-lived credentials

Looking Ahead - AI Adoption and NHI Security

Increase in ratio between human identities to NHI

Quick adoption leads to insecure authentication

Operate as their human means lack of accountability

AI on NHI creation, growth, and proliferation

AI on NHI orchestration, management, and security

Summary of the Survey

Main Takeaways

- Struggling with the basics of NHI security
  - Permissions and lifecycle management
- Challenges w/ Managing Permissions and API Keys
  - Applying least privilege to new and existing NHIs
- Fragmented Approaches Lead to Security Incidents
  - Unified strategies and policies
- High anxiety, low confidence when securing NHIs
  - Education, tools, community
- NHI security capabilities on the rise
  - Identify opportunities, solution awareness

Apply What You Have Learned Today

Next Steps

Next week:

- Inventorize existing User Service Accounts and third-party OAuth Applications

First 3 months:

- Define a provisioning process that includes:
  - Vaulting secrets
  - JML flow
  - Establish best-practices for NHI creation
- Transform User Service Accounts to credential-less NHIs (like managed identities)

Within 6 months:

- Include NHIs in your security awareness programs
- Implement minimal permissions engines (AWS Access analyzer, GCP Policy Intelligence)
- Create policies for third-party OAuth apps (Default - deny)

RSAC 2025 Conference

Thank you!

Q&A

The State of NHI Security

Many Voices.
One Community.